



Strategic Plan for Data Integration

October 2011

**North Carolina
Office of the State Controller**

David McCoy, State Controller

Executive Summary	1
North Carolina Strategic Plan for Data Integration	2
I. Introduction.....	2
II. Mission and Goals.....	4
A. Information Management Standardization	4
B. Data Management Standardization	4
C. Data Asset Optimization	4
D. Resource Development	4
E. Data Accessibility	4
III. Organization and Communication	4
A. Data Integration Steering Committee	5
B. Leadership Council	6
C. Data Integration Program Office	6
D. Project Team Members and User Groups	7
IV. Organization and Management	8
A. Program Oversight and Management	8
B. Data Governance.....	8
C. Application Life Cycle Development	9
D. Budget	10
E. Identify, Plan and Prioritize Opportunities	10
V. Technical Infrastructure	11
A. Production Environment	11
B. Database Platform	12
C. Common Technical Components.....	12
VI. Future Deliverables	13
A. Measurements of Success	13
B. Data Integration Program Initiatives.....	13
 <u>Appendix</u>	
Appendix 1: Session Law 2011, HB 200-145	14
Appendix 2: Application Life Cycle Development	18

Executive Summary

The North Carolina General Assembly ordered the preparation of this report and directed that it focus on Statewide Strategic Data Integration for state agencies and systems. The legislation targeted two areas: data integration and the development of a CJLEADS hosting and management services plan. Another report, issued concurrently with this one, reports on planning, programming, hosting, and management activities related to CJLEADS. The legislative history of the activity leading up to the mandate for the current report follows.

Session Law 2007-323, HB 1473 directed the Office of the State Controller (OSC), in cooperation with the State Chief Information Officer, to develop a Strategic Implementation Plan for the integration of databases and the sharing of information among state agencies and programs. In enacting this provision, the General Assembly's intent was to *"provide broad access to information across State government, and comply with all necessary security measures and restrictions to ensure that access to any specific information held confidential under federal and State law shall be limited to appropriate and authorized persons."*

In April 2008, the BEACON Strategic Plan for Data Integration was developed to establish a statewide program which promotes data warehousing and the use of analytics through standardized tools and provides secure access to reliable and accurate information. The Strategic Plan for Data Integration recognized the State's challenges with data siloed in disparate agency information systems and the need for a common, consistent standard on which to share information and allow the state to leverage its valuable data assets. The plan identified long-term goals and recommended a framework on which the data integration initiative could grow and realize its objective of transforming agencies' siloed data into meaningful statewide information to support quick, agile, event-driven analysis for business.

In early 2008, the deaths of two North Carolina university students highlighted the need for improved information sharing among the criminal justice community. The circumstances associated with these highly-publicized events drew attention to the tragic consequences when criminal justice professionals do not have quick, complete access to statewide offender information. In response to these events, **Session Law 2008-107, House Bill 2436** directed the OSC, in cooperation with the State Chief Information Officer (SCIO), and under the governance of the BEACON Project Steering Committee, to develop and implement a criminal justice data integration pilot program in Wake County. The goal of the pilot was to provide criminal justice professionals with access to timely, complete, and accurate information for enhanced decision making. The pilot program, Criminal Justice Law Enforcement Automated Data Services (CJLEADS), was the first major data integration initiative whose design and development efforts were guided by the 2008 Strategic Plan for Data Integration.

Session Law 2011-145, HB 200 directs the State Controller to continue the development of comprehensive enterprise-level data integration capability, providing broad access to and analysis of information across state government. Using the lessons learned from the CJLEADS project, knowledge of the current statewide infrastructure, and advances in technology, the OSC Data Integration Program Office has updated the North Carolina Strategic Plan for Data Integration.

North Carolina Strategic Plan for Data Integration

I. Introduction

Defining Data Integration

North Carolina's state agencies need to share information that has been collected between programs and between divisions within their own department, as well as with other agencies and governments within the State. In order to make informed decisions, legislators and the heads of the State's departments and agencies also need access to data information that has been collected by State agencies for analysis.

With the understanding that hindsight provides clarity—and had the State's decision makers had the benefit of know how technology would evolve—perhaps different decisions would have been made in the past. Today, however, we must work with the consequences of decisions that led to many of the systems supporting State agencies being developed in isolation of one another, often with incompatible technologies. The State has multiple independent systems that share many common data elements and serve overlapping bases but cannot communicate and share data with one another. Furthermore, these systems also support and sometimes require duplicate data entry, which hinders agency operations, utilizes limited resources, slows timely access, undermines the quality of the data, and the delivery of services.

Data integration encompasses a variety of functions designed to address many of these shortfalls while enabling timely and efficient sharing of information within and between departments, agencies, and governments. Statewide data integration is defined as the capability of merging and reconciling dispersed data for analytical purposes, through the use of standardized tools and with an infrastructure that supports quick, agile, event-driven analysis for business. The Plan does not strive to consolidate or address the issues associated with the disparate applications built to serve specific agency business functionality. Instead, it focuses on providing a secured flow of information from these applications to an integrated environment where statistical, analytical and predictive modeling can occur for improved enterprise business decisions.

In instituting a statewide enterprise-focused data integration effort, the State is seeking to eliminate duplicate data entry, provide access to information that is not otherwise available, enable the timely sharing of critical data, and promote the ability for State agencies to be more effective in coordinating service delivery with other State agencies or governments. In addition to improving the operational performance of State agencies, data integration enables the sharing of vital information among agencies involved in a service continuum related to the same purpose or outcome. Additionally, integrating data related to one segment of the population into alternative data sets or systems containing larger population segments, such as from the county to the State, helps optimize resources and eliminate redundant efforts undertaken toward the same outcome, e.g., fraud detection.

For the purposes of this report, the general definition of data integration is having the ability to access and share critical information, in near or real time, or at key decision points,

throughout the State's operational or service delivery process. As such, data integration efforts between a State agency's programs should include the ability to:

- Perform identity resolution at a satisfactory level of matching.
- Perform automatic queries across databases to review and evaluate results.
- Record or access information about agency services or transactions.
- Generate automatic alert notifications based on predetermined criteria.
- Request and receive information held by other agencies or distribute information, based on circulated lists of available information.

The implementation of an enterprise data integration effort is undertaken with the purpose of automating operations, reengineering systems and processes, and achieving new capabilities with greater efficiency and effectiveness. To accomplish the desired outcomes, the effort should capture data at, or as close to, the originating point as possible, rather than trying to reconstruct it or having others, at a later point in time, go through the effort to collect it again. Data should be captured once and used many times, leveraging existing resources and improving data quality. In addition, the integrated system should be driven by the operational systems of participating programs, not separate from the systems supporting the programs.

It is important to recognize that building integrated information systems does not mean that all information between programs is shared without regard to the data, the agencies or programs involved, or the sensitivity of the information. Often agencies or programs need to share sensitive information, on a need-to-know basis as authorized by statutes and rules, at or near real time, or at critical decision points throughout the agency's operational business process. To achieve maximum success, the North Carolina data integration effort should be grounded in a belief that the State's strategy should enable participating agencies to focus their operational efforts on their specific mission functions, to enhance their own information systems and to develop in scope and size without regard to the efforts or activities of other programs participating in the system. This data sharing approach is possible because participating programs retain stewardship and responsibility of the data in their area of the business and define which data they are able to share and the intended use of that data.

The underlying premise of the 2008 Strategic Plan for Data Integration was to start small, focus strategically and grow incrementally. It recognized that the statewide effort will evolve as the value proposition of data integration is realized. This report supports a plan with a phased approach where lessons learned from early adopters such as the CJLEADS project will guide and refine the evolution and implementation of North Carolina's data integration future.

Session Law 2011-145, HB 200 directs the State Controller to continue the development of comprehensive enterprise-level data integration capability, providing broad access to and analysis of information across state government. It further directs OSC to continue the deployment of the CJLEADS program and begin the development of a new data integration effort to support the identification of fraud, waste, and improper payments. The Data Integration Program Office under the direction of the State Controller will be guided by the 2011 North Carolina Strategic Plan for Data Integration in the continuous development of data integration programs.

II. Mission and Goals

The mission of the statewide data integration program is to maximize the use of the State's data assets for efficient and informed business decisions to improve business outcomes. To achieve this mission, the Strategic Plan for Data Integration sets forth a structured framework which fosters an environment of information accessibility and sharing to enable and promote the use of analytics for business decisions.

The long-term goals of the data integration initiative include:

A. Information Management Standardization

Statewide (enterprise) technology standards support data integration, reporting and analytics. Data analysis and business intelligence is conducted utilizing a common set of tools that offer scalability and flexibility.

B. Data Management Standardization

Statewide data identification and standardization are a common practice. Data is clearly defined, secured, and available via a common platform and toolset.

C. Data Asset Optimization

Data resources are stored and maintained centrally. Duplication of data for reporting is no longer common practice. Data use agreements between the owners and users are centrally managed.

D. Resource Development

Business owners and analysts are properly trained in the use of the analytical tools. Stakeholders collaborate and share best practices, techniques and lessons learned.

E. Data Accessibility

Information is available to authorized stakeholders where it is needed, when it is needed and to those who need it.

III. Organization and Communication

Communication and leadership are critical to successful data integration implementations. To achieve enterprise data integration, senior leadership must support and champion the movement while program committees guide and set direction, and project teams design, build and develop solutions. Open communication between these entities is the critical step in the development of sound analytical solutions.

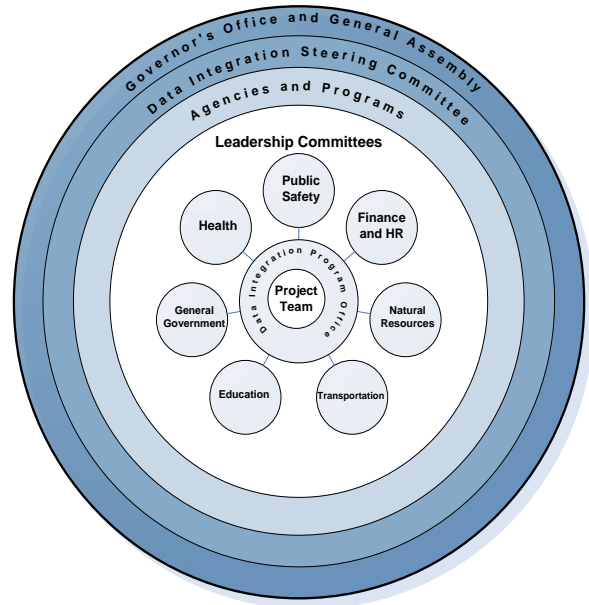
CJLEADS demonstrated strong communication and leadership. At each level of the organization those involved were engaged in the development effort. The lessons learned from the CJLEADS program will help guide the development of additional data integration programs.

Lesson Learned #1: Executive sponsorship and leadership must champion changes in business mindset from data ownership to data stewardship.

Lesson Learned #2: Feedback from business users is vital to ensure the business solutions developed support business analysis and decisions.

To encourage the necessary exchange of ideas in program development, the Strategic Plan for Data Integration encourages a communications hub that promotes collaboration. All levels of the organization work together in support of a common vision to improve business outcomes and decisions through effective, efficient and timely access to the State's data.

The State Controller will continue to foster cohesive communication among the various committees, groups and project team members.



A. Data Integration Steering Committee

The Data Integration Steering Committee, formed by the General Assembly in **Session Law 2011-145, HB200**, will help guide the statewide data integration efforts. This committee will be responsible for overseeing all data integration efforts in the State.

This Committee will be chaired by the State Controller and includes the following six voting members:

- One member with an information technology background and experience appointed by the Governor.
- One member with a background in law enforcement appointed by the Governor.
- One member with a background in government accounting appointed by the President Pro Tempore of the Senate.
- One member with government operations experience appointed by the President Pro Tempore of the Senate.
- One member with a background in information technology appointed by the Speaker of the House of Representatives.
- One member with a background in business management appointed by the Speaker of the House of Representatives.

The Director of the Office of State Budget and Management, the State Chief Information Officer, the State Treasurer, and the State Auditor will serve as advisory members.

B. Leadership Council

The Strategic Plan for Data Integration identifies the importance of communication and the active participation of leadership from all partner agencies and organizations. Together, members of the program leadership committees will help identify and prioritize solutions to meet the collective business needs of the partner organizations, based on time, resources and return on investment. With CJLEADS, the State Controller along with the Interagency Leadership Council, provided guidance, insight, and recommendations for the integration of criminal justice information.

Lesson Learned #3: A leadership council allows executive participation and interaction from partner organizations, sharing knowledge and expertise in support of a common goal.

As new data integration efforts evolve, collaborative leadership committees will be formed to support the development of enterprise solutions to meet specific business issues and needs.

C. Data Integration Program Office

The OSC Data Integration Program Office is based on an industry best practice which suggests the establishment of a Business Intelligence Competency Center (BICC) framework. In North Carolina, the OSC Data Integration Program Office supports a managed and organized approach toward data integration and the use of business intelligence. This program office provides a common consistent approach to data integration which allows stakeholders with interrelated disciplines, domains of knowledge, experiences and skills, to collaborate to promote data integration throughout the organization with a managed and structured technology approach.

CJLEADS leveraged the OSC Data Integration Program Office to assist in the ground up development and deployment of a data integration initiative. This program office demonstrated that with proper guidance and communication from data stakeholders, data integration solutions can be managed at the enterprise level.

Lesson Learned #4: Agency resources are best utilized when they focus strategically on the detailed business needs rather than technical development.

Lesson Learned #5: The establishment of an independent organization to support data integration solutions among various stakeholders provides an objective approach that encourages data stewardship instead of data ownership.

A BICC, like the OSC Data Integration Program Office, is a collaborative team that grows over time and matures with the organization's ability to promote and expand the use of business intelligence to drive strategic decisions. In most cases a mature competency center becomes a permanent organizational structure consisting of representatives from the business and IT communities. Together, they advance and promote business intelligence practices throughout the organization.

A primary goal of the OSC Data Integration Program Office is to encourage a cultural shift from siloed data ownership to enterprise data stewardship. As this cultural shift grows, the program office will support agencies in gaining insight into their informational needs through the application of data integration and analytics.

The OSC Data Integration Program Office will be comprised of a dedicated pool of experts, with proficiency in the technical use of analytics and its applicability to business. This team will serve as an internal consultative service to support agency and enterprise data integration and business intelligence initiatives. To fully establish this organization within the Office of the State Controller, budgetary funding separate from funding for specific initiatives is required to staff the program office with business analytics and technical expertise and to provide the capability for this organization to monitor business intelligence infrastructure and initiatives.

D. Project Team Members and User Groups

Each data integration initiative will be supported by project team members who represent both technical and business areas. These teams will be responsible for the development of applications to satisfy business needs in accordance with data and security standards. To ensure that each initiative represents the perspectives and needs of a wide variety of stakeholders, industry standards recommend that a community of interest comprised of partner agencies and programs, industry experts, and citizens work together to understand business issues and needs and make recommendations for appropriate solutions. When appropriate, this group may leverage panel discussions and focus groups with potential users, to meet, discuss and brainstorm solutions that will support their business decisions.

CJLEADS used the community of interest approach and involved representatives from the courts, corrections and law enforcement communities to help identify the data and decisions needed to support the criminal justice community. The CJLEADS application was developed iteratively and released in phases, allowing multiple project team members to participate in the design, development and implementation effort at different periods of time based upon their business expertise and the CJLEADS component being constructed.

Lesson Learned #6: Data integration project team members must have the knowledge and skill set needed to support the development of business rules incorporated into the application.

Lesson Learned #7: Project team members must be empowered to make decisions and/or have a direct communication line to the decision makers.

Project team members are critical to the successful deployment of data integration programs. Subject matter experts from partner agencies will provide vital business knowledge and skill to the development and design of business rules and application features. The OSC Data Integration Program Office will work closely with stakeholders to ensure project team resources are utilized efficiently and during appropriate times throughout the development effort.

IV. Organization and Management

To support the changing business needs it is critical that statewide data integration environments remain agile and focused on continuous improvement. As data integration promotes the accessibility of information for decision making, business processes will change, and additional information will be required to support the changing environment. To maintain a cycle of continuous improvement and to retain the value of the State's investment in data integration programs, a commitment is needed to support the management of the data integration program and the budgetary needs of the operations.

A. Program Oversight and Management

Industry standards suggest the incorporation of a Business Intelligence Competency Center where organizations with a business need can use the center's resources with knowledge and expertise to help guide them through leveraging data as business intelligence. The University of Michigan has deployed a successful Business Intelligence Center where all business owners and students can look toward this center for standards, tools and techniques in developing useful business information. This center has been in existence since 2004 and continues to be a valuable asset to their BI community.

In North Carolina, the OSC Data Integration Program Office implementation of CJLEADS was the first large-scale data integration initiative where data stewardship rather than data ownership was realized. By design, it re-thought the practice of duplication of data in each agency's environment and created a single repository where all users with the proper authorization can access the integrated data. This effort broke down the barriers of data ownership by developing data governance models, practices, and rules to support the dissemination of the State's data. It also changed the way in which project management and application life cycle development is traditionally approached. Rather than developing a large-scaled project with a single, predetermined implementation date forcing user agencies to adopt the project in its entirety, CJLEADS was developed and implemented in phases with new functionality and deliverables provided to end users in manageable stages.

For North Carolina to succeed with enterprise data integration efforts, it is recommended that the applications and technical infrastructure remain under the OSC Data Integration Program Office which will become an organization similar to the industry standard, BICC. Here, enterprise data integration, solutions, accessibility, and tools can be supported, enhanced and shared as business needs change. Business owners will become reliant on the OSC Data Integration Program Office to help them develop solutions by leveraging enterprise data.

B. Data Governance

The successful implementation of an enterprise data integration program requires business owners to understand the change in role of being a data owner to being a data steward. As a data steward, business leaders will be called upon to understand the importance of data and its value and impact on addressing business issues and problems. As a data steward, business owners and experts, must fully understand the regulatory rules that restrict data access while actively exploring new operational opportunities to securely share information to meet enterprise business needs.

During the CJLEADS initiative, business owners reviewed data collected within their operations and developed a governance model which enabled the sharing of necessary information in accordance with regulatory and statutory requirements. Each agency had unique business rules associated with the integration of its data. These requirements introduced governance practices including criminal background checks, nondisclosure agreements, memoranda of agreement, license and usage policies and strict user access and auditing tools.

Establishing a data governance model which supports the enterprise view of the organization is critical to the success of the data integration program. The CJLEADS initiative established a framework of policies, procedures and templates associated with data governance which can be leveraged and expanded as new stakeholders join the data integration movement.

Lesson Learned #8: Access to data sources and data quality can be challenging. Project team members with business knowledge must be available to support the development of data governance rules.

C. Application Life Cycle Development

Data integration and application development is by nature an iterative approach. Business needs change as new information emerges, and application development must be able to adapt and react in order to support more complex business decisions. Future enterprise initiatives will prove to be successful if the continuous process for improvement follows the CJLEADS life cycle development example as illustrated in Appendix 2.

With CJLEADS, the project team started with a pilot in Wake County. During the pilot, Wake County users provided feedback and evaluation of the application. This pilot period allowed validation, verification and modification of the application, policies and procedures prior to the delivery of the application statewide. Following the initial pilot, three planned phased releases have followed, with two additional phases in the development stage. For each release the new functionality offered is a direct result of initial business requirements as well user feedback on the need for expanded information to improve business decisions.

Lesson Learned #9: Planned incremental phased deliverables realizes benefits sooner and provided for the inclusion of user feedback into subsequent phases.

As the State progresses with the implementation of data integration solutions, the application solutions should be developed in a manner which offers flexibility and a managed iterative approach. All programs should consider a phased implementation where new modules can be introduced to improve business outcomes. The project team must remain responsive to changing business needs to ensure future development includes information needs.

D. Budget

To maintain an enterprise data integration program, recurring funding is required in support of the OSC Data Integration Program Office. This funding will support centralized personnel who provide consultation, guidance and technical expertise to on-going and future data integration initiatives. These personnel resources will ensure consistent standards, development approaches, governance and management of data sharing initiatives to support the State's enterprise business analytics and intelligences needs. Under the direction of the Data Integration Program Office, the application hosting and maintenance costs will be centrally managed and costs will be shared across all data integration programs. The Data Integration Program will remain focused on effective cost management through shared infrastructure, shared technology development and consolidated data.

Funds must also be identified to ensure the investments made to support data integration, and business analytic development is protected with recurring financial resources to manage on-going operations and to support program enhancements critical to providing continuous improvement. As realized with the CJLEADS program, application and technical improvements continue to be communicated with executive management, thus, new data and functional points are regularly prioritized and implemented. In accordance with **Session Law 2011-145, HB200**, the Data Integration Steering Committee will provide guidance to the prioritization and budgeting requirements of the program.

E. Identify, Plan and Prioritize Opportunities

Within the public sector, there is an unlimited list of opportunities associated with enterprise data integration and the application of data analytics. For example, business intelligence can be used to improve the State's ability to make decisions, respond to constituents needs, measure performance, shift users toward self-service, decrease costs and improve operational efficiency. The solutions developed may include summary information on a dashboard, performance scorecards, case management, predictive analysis, fraud detection, risk analysis, GIS mapping, financial analysis, reporting and tracking.

The challenge for North Carolina will be to identify and develop solutions which meet the agencies' immediate needs and support the State's long-term integration vision. Ideally, the strategic projects identified and the solutions developed will be more enterprise-focused and less siloed.

Senior management will be engaged to champion business analytics and data sharing. Their direct involvement will provide the necessary leadership to encourage the cultural shift toward data stewardship. With their guidance, stakeholders will outline their business issues and challenges, and will work collaboratively to identify the information and analytics that can be leveraged to meet the need and improve the decision-making process.

Open communication will be critical in developing sound analytical solutions. To encourage the necessary exchange of ideas, the Office of the State Controller will foster collaborative teams around the common areas of interest (e.g. finance, budget, public

safety, health, transportation, etc.). These leadership committees will engage agencies, programs, citizens, and industry experts in a collaborative forum to understand the issues and needs. Together, they will plan, prioritize and develop solutions to achieve the greatest return on investment.

V. Technical Infrastructure

A technical infrastructure with a common toolset where data, programming and best practices can be shared is critical to successful enterprise data integration. The development of a comprehensive statewide data integration capability requires a technical foundation which ensures accessibility, interoperability, security and transparency.

A. Production Environment

A production data center environment provides a secure and reliable hosting facility to support the day-to-day operations of the application as well as to ensure the appropriate level of service, hardware and software support/maintenance, and continuity of business operations. The establishment of a robust technical environment can be costly. If technical environments are architected for scalability, however, the environment can grow and expand to support new business data and functional features at a much smaller cost than establishing a separate environment for each business area.

The 2008 Strategic Plan for Data Integration recommended leveraging the State's Enterprise Licensing Agreement (ELA) with the State's data integration vendor and where appropriate, the State's Enterprise Data Warehouse (EDW). Over time, the EDW, an expensive and under-utilized enterprise service hosted at ITS, was discontinued. The specific technical skills needed to manage the environment were challenging to maintain and agencies failed to fully embrace the service offering.

When the CJLEADS data integration initiative began, the legislature set forth an aggressive timeline to implement the initial application prototype. To meet this timeline, OSC leveraged the State's data integration vendor to establish and host a technical environment and develop a state-of-the-art criminal justice application. SAS worked with the State to establish a technical environment to support 24x7x365 hours of operation for 33,000 users.

Based on the successful deployment and management of the CJLEADS program in the vendor-hosted environment, the new initiative to implement an enterprise fraud, waste, and improper payment detection program also will be hosted at the vendor data center environment. The ability to host multiple data integration applications in a common environment will improve the ability to share information, leverage common infrastructure and technical skills and potentially reduce costs by more fully utilizing hardware for multiple projects.

Lesson Learned #10: A common technical platform which enables the sharing of data must be established.

Lesson Learned #11: State tools, infrastructure and enterprise agreements should be leveraged to maximize the return on investment.

B. Database Platform

Data integration relies on the accessibility of the State's enterprise data. A single repository platform should be promoted to leverage economies-of-scale and interoperability. This platform must ensure data standards, security and accessibility. CJLEADS data and application is hosted at the State's data integration vendor, SAS, and was developed using SAS data integration and analytical tools. This effort compiles 42 million records, spanning over 20 years of information, in an integrated database that provides comprehensive views of offender activity, automated alerting process, and analytical reports.

A common database platform is integral to data integration and interoperability. The common platform allows the State to collect data available from disparate applications, and transform the data into quality, consistent, and meaningful information which can be shared among the enterprise. The common platform also enables standard programming techniques to extract, transform, and load data, to create reports, and to share code, common data definitions, and improved data quality.

During the integration of data for the CJLEADS application, the project team found that the data's age, inconsistent formats, and varying quality of source information impacted the approach to extracting, transforming and loading data into the CJLEADS databases. Shared database technology and experience with the State's data assets will improve the ability to interpret data and transform it into common, consistent formats available to meet the State's business analytics and reporting needs.

Lesson Learned #12: The quality of the data in existing legacy applications is sometimes suspect and requires special business rules when loading the data warehouse.

C. Common Technical Components

Common technical components allow the state to leverage the shared capabilities to secure and track access to information. The data accessible in the CJLEADS application has strict security requirements. User access and authentication was developed by leveraging the State's standard identity management system and developing an application specific role-based security feature which allows users who have authorization to see sensitive information. In addition, CJLEADS developed a robust auditing capability to track and report all user activity. This information will be leveraged to complete annual audits, investigate potential misuse of the system and report overall system usage statistics.

CJLEADS has developed many application features which can be leveraged in the development of future enterprise data integration activities.

Lesson Learned #13: Leveraging existing application features such as the state authentication model, NCID, provided users with a common userid and password and eliminated the additional cost associated with the development of a standalone solution.

VI. Future Deliverables

A. Measurements of Success

The long-term vision of statewide data integration is to maximize the State's data assets for efficient and informed business decisions on which the outcomes can be monitored and acted upon. The critical success factors associated with this effort include; cultural transformation, policy alignment, governance and standards, resource availability, cross-agency communication, and technology support. With guidance from the legislature, the Data Integration Steering Committee and program leadership teams, as well as the OSC Data Integration Program Office will evaluate performance outcomes to identify areas where data integration should be expanded to support the growing needs.

The OSC Data Integration Program Office will be responsible for the development of performance measures associated with the data integration programs. The performance of the programs will be measured against the mission and goals of data integration. Performance measurement also will be developed at the project level by the stakeholders involved in the development of business intelligence applications, to report the success of their data integration effort and identify areas for continuous improvement. The Data Integration Program Office will report each program's performance in regular reports to the Legislature, Data Integration Steering Committee, executive management and the individual program leadership committees.

B. Data Integration Program Initiatives

Session Law 2011-145, HB 200 has directed the Office of the State Controller to continue the implementation of the CJLEADS application and to initiate the development of a comprehensive enterprise-level data integration framework to support the detection of fraud, waste, and improper payments.

The data integration initiative for fraud will follow a similar approach to the development effort of CJLEADS. Unlike CJLEADS where the focus was on a particular business area, criminal justice, the fraud framework will present a unique challenge with the broad scope of potential business areas. While the project must be developed to include a wide scope of business data, appropriate controls must be developed to ensure the data is integrated and secured among the various business areas of interest. For example, financial, insurance and service delivery fraud may share some common data sources; however, there may be application-specific data that will be accessible only to the investigator associated with that particular business objective. The lessons learned and the governance practices implemented during the CJLEADS development provides a framework upon which complex business rules can be cultivated to support information sharing across disparate lines of business.

As the data integration program begins development on the fraud initiative, the OSC Data Integration Program Office will evaluate the technical infrastructure and ensure the capability of information sharing between CJLEADS and the fraud initiative.

The strategic plan for data integration will provide the basis upon which the fraud initiative will be developed.

Appendix 1: Session Law 2011, HB 200-145

CJLEADS

CRIMINAL JUSTICE LAW ENFORCEMENT AUTOMATED DATA SERVICES (CJLEADS)

SECTION 6A.4.(a) The Office of the State Controller, in cooperation with the State Chief Information Officer, shall:

- (1) Continue the implementation of the Criminal Justice Data Integration Pilot Program, which is now known as the Criminal Justice Law Enforcement Automated Data Services (CJLEADS), expanding it throughout the State of North Carolina;
- (2) Review plans to transition CJLEADS to the Department of Justice, determining if that is still the best course of action, and identifying an alternative, if required;
- (3) By October 1, 2011, provide a recommendation to the Joint Legislative Oversight Committee on Information Technology on the best alternative for managing and hosting CJLEADS, along with a time line for the transition; and
- (4) Provide quarterly reports on the status of the Program to the Joint Legislative Oversight Committee on Information Technology beginning October 1, 2011.

SECTION 6A.4.(b) The Office of the State Controller shall administer CJLEADS with the assistance of a Leadership Council consisting of:

- (1) The Attorney General;
- (2) The Director of the Administrative Office of the Courts;
- (3) The Secretary of the Department of Correction;
- (4) The Secretary of Crime Control and Public Safety;
- (5) The Secretary of the Department of Juvenile Justice and Delinquency Prevention;
- (6) The Commissioner of Motor Vehicles, Department of Transportation;
- (7) The President of the North Carolina Association of Chiefs of Police;
- (8) The President of the North Carolina Sheriffs' Association, Inc.;
- (9) A representative of the Federal Bureau of Investigation, who shall be a nonvoting member;
- (10) The State Controller; and
- (11) The State Chief Information Officer.

SECTION 6A.4.(c) Data that is not classified as a public record under G.S. 132-1 shall not be considered a public record when incorporated into the CJLEADS database.

SECTION 6A.4.(d) To maintain the confidentiality requirements attached to the information provided to CJLEADS by the various State and local agencies, each source agency providing data for CJLEADS shall be the sole custodian of the data for the purpose of any request for inspection or copies thereof under Chapter 132 of the General Statutes. CJLEADS shall only allow access to data from the source agencies in accordance with rules adopted by the respective source agencies.

SECTION 6A.4.(e) Agencies shall use existing resources to provide required support for CJLEADS.

SECTION 6A.4.(f) Section 6.10 of S.L. 2010-31 is repealed.

Session Law 2011, HB 200-145 (continued)

Data Integration

COMPREHENSIVE ENTERPRISE-LEVEL DATA INTEGRATION CAPABILITY

SECTION 6A.20.(a)

The Office of the State Controller (OSC) shall continue the development of a comprehensive enterprise-level data integration capability, providing broad access to and analysis of information across State government. As part of this development effort, by October 1, 2011, OSC shall update the BEACON Strategic Plan for Data Integration and shall provide the updated plan to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly. The priority of effort for data integration shall be the Criminal Justice Law Enforcement Automated Data System (CJLEADS).

The strategic plan shall comply with all necessary security measures and restrictions to ensure that access to any specific information held confidential under federal or State law shall be limited to appropriate and authorized persons. OSC shall also develop, document, and enforce security requirements for data integration initiatives, to include establishing and monitoring security standards for vendors supporting development and implementation efforts.

SECTION 6A.20.(b) There is created a Data Integration Steering Committee that shall have responsibility for overseeing all data integration efforts in the State. This Committee shall assume all of the BEACON Project Steering Committee roles and responsibilities for oversight of data integration projects. This Committee shall be chaired by the State Controller and shall include the following six voting members:

- (1) One member appointed by the Governor with an information technology background and experience.
- (2) One member appointed by the Governor with a background in law enforcement.
- (3) One member appointed by the President Pro Tempore of the Senate with a background in government accounting.
- (4) One member appointed by the President Pro Tempore of the Senate with government operations experience.
- (5) One member appointed by the Speaker of the House of Representatives with a background in information technology.
- (6) One member appointed by the Speaker of the House of Representatives with a background in business management.

Members shall not have any association with potential vendors.

The Director of the Office of State Budget and Management, the State Chief Information Officer, the State Treasurer, and the State Auditor shall serve as advisory members.

The Committee shall be housed in and supported by the Office of the State Controller.

Session Law 2011, HB 200-145 (continued)

Fraud Detection

SECTION 6A.20.(c) As part of the State's continuing effort to develop a comprehensive enterprise-level data integration capability, the Office of the State Controller shall develop an enterprise process to detect fraud, waste, and improper payments across State agencies. State agencies shall fully support and participate in OSC's efforts to develop an automated fraud detection system

In support of the automated fraud detection effort, the OSC shall:

- (1) Develop a detailed long-range plan to implement an automated fraud detection system within State agencies.
- (2) Determine costs, to include vendor costs, for the effort for five years, beginning July 1, 2011.
- (3) Coordinate with State agencies to determine interest in participating in the project and to identify potential applications that can be included in an initial request for proposal.
- (4) Establish priorities for developing and implementing potential applications.
- (5) Evaluate savings resulting from each effort.
- (6) Coordinate efforts with the State's data integration vendor to begin the implementation process.
- (7) Establish a pilot to begin the implementation process and to identify and resolve issues associated with expansion of the initiative.
- (8) Coordinate with participating agencies to ensure that each has the resources and processes necessary to follow up on incidents of fraud identified by the vendor.
- (9) Provide recommendations to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly on potential future initiatives and the cost and savings associated with each.

SECTION 6A.20.(d) Beginning October 1, 2011, the OSC shall provide quarterly reports to the chairs of the Appropriations Committee of the House of Representatives and the Appropriations/Base Budget Committee of the Senate, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly. These reports shall include the following:

- (1) Incidents, types, and amounts of fraud identified, by agency.
- (2) The amount actually recovered as a result of fraud identification, by agency.
- (3) Agency procedural changes resulting from fraud identification and the time line for implementing each.
- (4) State costs for fraud detection for the previous quarter.
- (5) Payments to the vendor for the previous quarter.
- (6) Anticipated costs and vendor payments for each of the next two years from the date of the report.

SECTION 6A.20.(e) The Office of the State Controller is authorized to enter into an enterprise automated fraud detection contract for eight million dollars (\$8,000,000) for a two-year contract period. Under the terms of the contract, payments are limited to the following payment schedule:

- (1) December 2011—\$1,000,000.
- (2) July 2012—\$3,000,000.
- (3) December 2012—\$3,000,000.
- (4) June 2013—\$1,000,000.

Further, payments shall be contingent upon achieving the anticipated schedule of benefits realization.

To maximize cost reductions and savings, the Office of the State Controller shall enter into the agreement no later than September 1, 2011. To ensure this is a Public-Private Partnership, the Office of the State Controller shall ensure that the chosen vendor shall contribute resources valued at least five million dollars (\$5,000,000) during each of fiscal year 2011-2012 and fiscal year 2012-2013 for the project's success.

SECTION 6A.20(f) The Office of State Controller shall ensure that the State receives an appropriate share of intellectual property ownership or residuals, or both, accruing as a result of subsequent contracts between the vendor and third parties that utilize the innovations developed as a result of this contract.

SECTION 6A.20(g) Of the funds appropriated from the General Fund to the Office of the State Controller, the sum of one million five hundred thousand dollars (\$1,500,000) for the 2011-2012 fiscal year and the sum of seven million five hundred thousand dollars (\$7,500,000) for the 2012-2013 fiscal year shall be used to support the enterprise process to detect fraud, waste, and improper payments across State agencies in each year of the biennium. Of these funds, five hundred thousand dollars (\$500,000) each year shall be used by the Office of the State Controller to support the initiative. The remainder may be used to fund payments to the vendor.

Session Law 2011-391, HB 22 (Technical Corrections Bill)

SECTION 12.(c) Section 6A.20(c) of Session Law 2011-145 reads as rewritten:

"**SECTION 6A.20.(c)** As part of the State's continuing effort to develop a comprehensive enterprise-level data integration capability, the Office of the State Controller shall develop an enterprise process to detect fraud, waste, and improper payments across State agencies. State agencies shall fully support and participate in OSC's efforts to develop an automated fraud detection system and shall upon request provide in a timely and responsive manner accurate, complete, and timely data, business rules and policies, and support for project requirements. The agency head shall verify, in writing, the accuracy, completeness, and timeliness of the data. If any support or data is not provided as needed for the automated fraud detection effort, the OSC shall report that failure to the General Assembly for further review and action.

In support of the automated fraud detection effort, the OSC shall:

- (1) Develop a detailed long-range plan to implement an automated fraud detection system within State agencies.
- (2) Determine costs, to include vendor costs, for the effort for five years, beginning July 1, 2011.
- (3) Coordinate with State agencies to determine interest in participating in the project and to identify potential applications that can be included in an initial request for proposal.
- (4) Establish priorities for developing and implementing potential applications.
- (5) Evaluate savings resulting from each effort.
- (6) Coordinate efforts with the State's data integration vendor to begin the implementation process.
- (7) Establish a pilot to begin the implementation process and to identify and resolve issues associated with expansion of the initiative.
- (8) Coordinate with participating agencies to ensure that each has the resources and processes necessary to follow up on incidents of fraud identified by the vendor.
- (9) Provide recommendations to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly on potential future initiatives and the cost and savings associated with each."

Appendix 2: Application Life Cycle Development

This graphic illustrates the application development lifecycle for the CJLEADS data integration initiative. The lessons learned from this effort will help develop and shape future enterprise initiatives. Critical to the success of CJLEADS was an iterative development approach, where deliverables are staged to allow for user feedback. In this depiction, the present state of CJLEADS identifies the need for the integration of federal data, the integration of the State facial recognition program and the development of a smart phone mobile application platform for use by officers.

